IN THE FOREIGN INTELLIGENCE SURVEILLANCE COURT

In re: Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act	No. 105B(g) 07-01

REPLY IN SUPPORT OF YAHOO! INC.'S MOTION UNDER FISC RULE 62

The Government has informed Yahoo! Inc. ("Yahoo!"), through its pleadings and otherwise, that Yahoo!'s name and its counsels' identities are no longer classified and may be released immediately. The Government has not objected to Yahoo!'s request for a new classification review and release of this Court's order and the parties' briefs. Yahoo! therefore asks this Court to enter an order:

A. Stating the Court does not object to release of all of its orders or the parties' briefing; and

B. Directing the government to conduct a classification review of this Court's orders and briefing this matter for public release.

See Ex. A, *In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act,* No. 08-01, Order (For. Intel. Surv. Ct. of Rev. June 28, 2013).

ARGUMENT

Release of this Court's decision and the parties' briefing is necessary to inform the growing public debate about how this Court considers and examines the Government's use of directives. Courts have long recognized the public has a right to access court records. *United States v. Mitchell*, 551 F.2d 1252, 1258 (D.C. Cir. 1976), *rev'd on other grounds sub nom. Nixon v. Warner Commc'ns, Inc.*, 435 U.S. 589 (1978) (The common law access right "is not some arcane relic of ancient English law," but rather "is fundamental to a democratic state.") "There is a 'strong presumption in favor of public access to judicial proceedings.'" *In re Sealed Case*, 237 F.3d 657, 666 (D.C. Cir. 2001) (*citing Johnson v. Greater Southeast Cmty. Hosp. Corp.*, 951 F.2d 1268, 1277 (D.C. Cir. 1991)). Executive Order 13,526 also recognizes that "the need to protect [classified] information may be outweighed by the public interest in disclosure of the information, and in these cases the information should be declassified."

Following these principles, the Foreign Intelligence Surveillance Court of Review ("FISCR") accepted the need for additional public access to court records in this case. *See* Ex. A, *In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act,* No. 08-01, Order (For. Intel. Surv. Ct. of Rev. June 28, 2013). The FISCR recognized that since it decided this case, "more than four years have passed, and recent events suggest that there may have been a change in

the government's position as to what it considers classified in this matter." *Id.* at 2-3. The FISCR thus held that "it is appropriate for this Court to order the requested relief and not to require the Provider to initiate a separate proceeding under the Freedom of Information Act." *Id.* at 3. It ordered the Government, by July 12th, to provide a timeline for declassifying additional portions of its decision and the parties' legal briefs for this case on appeal. *Id.* This Court should do the same with regard to the previously unreleased record in this case, including the decision compelling Yahoo! to comply, the Court's denial of Yahoo!'s request for a stay, and the parties' briefing.

The directives at issue in this case are at the center of a robust national debate represented by countless news articles, a statement from the Director of National Intelligence,[1] and congressional hearings.[2] Providing more information about the methods the government uses, the arguments this Court considers, and the Court's reasoning would inform this debate and prevent misunderstandings

---

[1] Ex. B., James Clapper, *DNI Statement on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (June 8, 2013) *available at* http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/872-dni-statement-on-the-collection-of-intelligence-pursuant-to-section-702-of-the-foreign-intelligence-surveillance-act.

[2] U.S House of Representatives Permanent Select Committee on Intelligence, *How Disclosed NSA Programs Protect Americans, and Why Disclosure Aids our Adversaries* (June 18, 2013), *recording available at* http://www.ustream.tv/recorded/34527763. Ex. C, U.S House of Representatives Permanent Select Committee on Intelligence, *How Disclosed NSA Programs Protect Americans, and Why Disclosure Aids our Adversaries*, Opening Statement of Chairman Rogers' (June 18, 2013) *available at* http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/ChairOpening06182013.pdf

based on incomplete information.[3] As Representative Rogers, Chairman of the U.S House of Representatives Permanent Select Committee on Intelligence stated, "One of the more damaging aspects of selectively leaking incomplete information is that it paints an inaccurate picture and fosters distrust in our government." Ex. D at 1. This Court's thorough analysis of Yahoo!'s objections, and arguments in the parties' briefs, would allow the public to observe the process by which this Court oversees directives, and offer more complete information about that process, while still protecting classified information. *See, e.g., Richmond Newspapers, Inc. v. Virginia*, 448 U.S. 555, 572 (1980) (noting that in criminal cases "the appearance of justice can best be provided by allowing people to observe it.")

Other parties are also demanding information from Yahoo! (and other providers) about their responses to directives. Plaintiffs have already filed lawsuits against providers, including Yahoo!, that news reports have characterized as having responded to directives and/or taken part in the PRISM program. *See, e.g., Klayman v. Obama*, No. 13-cv-00881-RJL (D.D.C. filed June 11, 2013). Yahoo!, like other electronic communications providers, is under public pressure to provide more information about its responses to United States Government demands for user data. Disclosure of the directives and the briefs in this case would also allow

[3] *See, e.g.*, Ex. D, Eric Lichtblau, *In Secret, Court Vastly Broadens Powers of N.S.A.*, The New York Times (July 6, 2013) http://www.nytimes.com/2013/07/07/us/in-secret-court-vastly-broadens-powers-of-nsa.html?pagewanted=all&_r=0 (revealing a lack of clarity arising from incomplete release of court opinions).

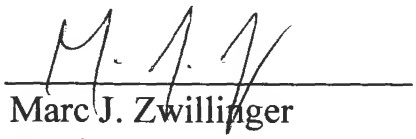
Yahoo! to demonstrate that it objected strenuously to the directives that are now the subject of debate, and objected at every stage of the proceeding, but that these objections were overruled and its request for a stay was denied. Most importantly, making this Court's thorough analysis available to the public will provide the public with valuable information about how the parties and the Court vetted the Government's arguments supporting the use of directives. That information will give the public a more complete understanding of the directive process, allowing U.S. citizens to inform their legislative representatives as to their views on the continued use of the directive process, especially as the statutes authorizing directives are up for reauthorization. Pub. L. 112-238, § 2(a)(1) (reauthorizing directives until December 31, 2017). In short, additional disclosures will advance the proper functioning of our representative democracy with regard to the statute that authorizes the use of directives. *See, e.g.*, *Richmond Newspapers*, 448 U.S. at 572; *Minneapolis Star and Tribune Co. v. Minnesota Comm'r of Revenue*, 460 U.S. 575, 585 (1983) ("an informed public is the essence of working democracy.").

CONCLUSION

Given the Government's decision not to object to the relief Yahoo! has requested, and its declassification of Yahoo!'s identity, Yahoo! asks this Court to enter an order:

1. Stating that the Court does not object to release of all of its orders in this case or the parties' briefing; and
2. Directing the government to conduct a classification review of the orders and briefing in this matter for public release.

Dated: July 9, 2013

Signature: 

Marc J. Zwillinger
Jacob A. Sommer
ZwillGen PLLC
1705 N St. NW
Washington, DC 20036
marc@zwillgen.com
jake@zwillgen.com
Attorneys for Yahoo! Inc.

CERTIFICATE OF SERVICE

I hereby certify that on July 9, 2013, I served copies of the foregoing motion on:

Carli Rodriguez-Feo
United States Department of Justice
Litigation Security Group
2 Constitution Square
145 N St NE
Suite 2W-115
Washington, D.C. 20530
(202) 514-9016
Carli.Rodriguez-Feo@usdoj.gov

pursuant to FISC Rule 8 and procedures established by the Security and Emergency Planning Staff, United States Department of Justice.

Sean T. Moran

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE

COURT OF REVIEW

WASHINGTON, D.C.

IN RE DIRECTIVES PURSUANT TO SECTION 105B OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT.	)	Docket No. 08-01

ORDER

This matter is before the Court on the Motion of the Provider to "Publish Additional Portions of the Court's Decision" in In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004 (Foreign Intel. Surv. Ct. of Rev. 2008), which was submitted on June 14, 2013.[1] The U.S. Department of Justice filed a response to the motion on June 25, 2013, and the Provider waived its right to reply on June 26, 2013.

The Provider moves this Court to issue an order stating: "(1) that it does not object to the Government's release of additional portions of its opinion in this case and (2) directing the Government to revisit its classification decisions under Executive Order 13,526 to determine if classification remains appropriate in light of recent disclosures." Mot. at 8 (footnote omitted). Earlier in its filing, the Provider requested that this Court "publish additional information including, but not limited to, the identity of the Provider and its counsel and the arguments made

[1] Provider styles its pleading as request for relief under Foreign Intelligence Surveillance Court (FISC) Rule 62. As a matter of clarification, Rule 62 applies to the FISC only, and not this Court.

in the briefs." Id. at 1. The government, in its response, does not oppose the relief sought or object to the Provider's requests. Resp. at 1-2. With respect to the Provider's request that this Court state that it does not object to the government's release of additional portions of its August 22, 2008, opinion in this case, the government takes no position. With respect to the identity of the Provider and the contents of the present motion and response, the government states that "the identity of the petitioner in the 2008 litigation can now be declassified" and that it had no objection to the Motion being made publicly available. Id. at 2-3. With respect to the request for a new classification review, the government states that it does not object to the request, although it contends that it is not necessary for the Court to direct that relief, which could be triggered by a request under the Freedom of Information Act.

This Court's January 12, 2009, Order places under seal all classified information in this matter. 551 F.3d at 1017. That Order defines "classified information" as "any information, document, or portion of a document, not included in the published, redacted opinion, that has been and remains classified by an Executive Branch agency or official pursuant to applicable Executive Orders...." Id. In light of the government's Response, this Court no longer considers the identities of the Provider or its counsel to be covered by this Court's sealing order.

This Court stated in its January 12, 2009, Order that "[i]t would serve the public interest and the orderly administration of justice to publish" the August 22, 2008, Opinion, but that "an unredacted opinion would disclose materials that have been properly classified by the Executive Branch." 551 F.3d at 1016. As a result, redactions were made to the Court's opinion in consultation with the Executive Branch prior to publication. Since that time, more than four years have passed, and recent events suggest that there may have been a change in the

government's position as to what it considers classified in this matter. In recognition of this Court's authority over its own records and files, the Court concludes that it is appropriate for this Court to order the requested relief and not to require the Provider to initiate a separate proceeding under the Freedom of Information Act.

For the reasons discussed above, this Court rules that it does not object to the government's release of additional portions of the Court's August 22, 2008, Opinion in this case to the extent that the government concludes that those matters may be declassified. In addition, IT IS HEREBY ORDERED that the government is to conduct a new classification review of the following:

1. This Court's August 22, 2008, Opinion in this matter.

2. The Parties' Legal Briefs in this matter.

The government is to report back to the Court by July 12, 2013, with estimated dates by which it will be able to complete its review of the two categories of information indicated above.

SO ORDERED, this 28th day of June, 2013.

WILLIAM C. BRYSON
Judge, United States Foreign
Intelligence Surveillance
Court of Review

DNI Statement on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act

DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

June 8, 2013

DNI Statement on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act

Over the last week we have seen reckless disclosures of intelligence community measures used to keep Americans safe. In a rush to publish, media outlets have not given the full context–including the extent to which these programs are overseen by all three branches of government–to these effective tools.

In particular, the surveillance activities published in The Guardian and The Washington Post are lawful and conducted under authorities widely known and discussed, and fully debated and authorized by Congress. Their purpose is to obtain foreign intelligence information, including information necessary to thwart terrorist and cyber attacks against the United States and its allies.

Our ability to discuss these activities is limited by our need to protect intelligence sources and methods. Disclosing information about the specific methods the government uses to collect communications can obviously give our enemies a "playbook" of how to avoid detection. Nonetheless, Section 702 has proven vital to keeping the nation and our allies safe. It continues to be one of our most important tools for the protection of the nation's security.

However, there are significant misimpressions that have resulted from the recent articles. Not all the inaccuracies can be corrected without further revealing classified information. I have, however, declassified for release the attached details about the recent unauthorized disclosures in hope that it will help dispel some of the myths and add necessary context to what has been published.

James R. Clapper, Director of National Intelligence

DIRECTOR OF NATIONAL INTELLIGENCE

WASHINGTON, DC 20511

June 8, 2013

Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act

- PRISM is not an undisclosed collection or data mining program. It is an internal government computer system used to facilitate the government's statutorily authorized collection of foreign intelligence information from electronic communication service providers under court supervision, as authorized by Section 702 of the Foreign Intelligence Surveillance Act (FISA) (50 U.S.C. § 1881a). This authority was created by the Congress and has been widely known and publicly discussed since its inception in 2008.

- Under Section 702 of FISA, the United States Government does not unilaterally obtain information from the servers of U.S. electronic communication service providers. All such information is obtained with FISA Court approval and with the knowledge of the provider based upon a written directive from the Attorney General and the Director of National Intelligence. In short, Section 702 facilitates the targeted acquisition of foreign intelligence information concerning foreign targets located outside the United States under court oversight. Service providers supply information to the Government when they are lawfully required to do so.

- The Government cannot target anyone under the court-approved procedures for Section 702 collection unless there is an appropriate, and documented, foreign intelligence purpose for the acquisition (such as for the prevention of terrorism, hostile cyber activities, or nuclear proliferation) and the foreign target is reasonably believed to be outside the United States. We cannot target even foreign persons overseas without a valid foreign intelligence purpose.

- In addition, Section 702 cannot be used to intentionally target any U.S. citizen, or any other U.S. person, or to intentionally target any person known to be in the United States. Likewise, Section 702 cannot be used to target a person outside the United States if the purpose is to acquire information from a person inside the United States.

- Finally, the notion that Section 702 activities are not subject to internal and external oversight is similarly incorrect. Collection of intelligence information under Section 702 is subject to an extensive oversight regime, incorporating reviews by the Executive, Legislative and Judicial branches.

- *The Courts.* All FISA collection, including collection under Section 702, is overseen and monitored by the FISA Court, a specially established Federal court comprised of 11 Federal judges appointed by the Chief Justice of the United States.
    - The FISC must approve targeting and minimization procedures under Section 702 prior to the acquisition of any surveillance information.
        - Targeting procedures are designed to ensure that an acquisition targets non-U.S. persons reasonably believed to be outside the United States for specific purposes, and also that it does not intentionally acquire a communication when all the parties are known to be inside the US.
        - Minimization procedures govern how the Intelligence Community (IC) treats the information concerning any U.S. persons whose communications might be incidentally intercepted and regulate the handling of any nonpublic information concerning U.S. persons that is acquired, including whether information concerning a U.S. person can be disseminated. Significantly, the dissemination of information about U.S. persons is expressly prohibited unless it is necessary to understand foreign intelligence or assess its importance, is evidence of a crime, or indicates a threat of death or serious bodily harm.

- *The Congress.* After extensive public debate, the Congress reauthorized Section 702 in December 2012.
    - The law specifically requires a variety of reports about Section 702 to the Congress.
        - The DNI and AG provide exhaustive semiannual reports assessing compliance with the targeting and minimization procedures.
        - These reports, along with FISA Court opinions, and a semi-annual report by the Attorney General are provided to Congress. In short, the information provided to Congress by the Executive Branch with respect to these activities provides an unprecedented degree of accountability and transparency.
    - In addition, the Congressional Intelligence and Judiciary Committees are regularly briefed on the operation of Section 702.

- *The Executive.* The Executive Branch, including through its independent Inspectors General, carries out extensive oversight of the use of Section 702 authorities, which includes regular on-site reviews of how Section 702 authorities are being implemented. These regular reviews are documented in reports produced to Congress. Targeting decisions are reviewed by ODNI and DOJ.

    - Communications collected under Section 702 have provided the Intelligence Community insight into terrorist networks and plans. For example, the Intelligence

Community acquired information on a terrorist organization's strategic planning efforts.

- Communications collected under Section 702 have yielded intelligence regarding proliferation networks and have directly and significantly contributed to successful operations to impede the proliferation of weapons of mass destruction and related technologies.
- Communications collected under Section 702 have provided significant and unique intelligence regarding potential cyber threats to the United States including specific potential computer network attacks. This insight has led to successful efforts to mitigate these threats.

· The Committee will come to order.

· General Alexander, Deputy Attorney General Cole, Deputy Director Joyce and Mr. Litt, thank you for appearing before us today—especially on short notice.

· The Ranking Member and I believed it was important to hold an open hearing today to provide this House and the public with an opportunity to hear directly from you how the Government is using the legal authorities that Congress has provided to the Executive Branch since the terrorist attacks of September 11, 2001.

· I also would like to recognize the hard work of the men and women of the NSA and the rest of the IC who work day in and day out to disrupt threats to our national security. The people at NSA, in particular, have heard a constant public drumbeat about a laundry list of nefarious things they are alleged to be doing to spy on Americans. Yet, they keep their heads down and keep working every day to keep us safe. General Alexander, please convey our thanks to your team.

· This Committee has been extensively briefed on these efforts on a regular basis as part of our ongoing oversight responsibility over the 16 elements of the Intelligence Community and the National Intelligence Program.

· In order to fully understand intelligence collection programs, most of these briefings and hearings have taken place in classified settings. Nonetheless, the collection efforts under the business records provision and Section 702 of FISA are legal, court-approved and are subject to an extensive oversight regime.

· I look forward to hearing from all of the witnesses about the extensive protections and oversight in place for these programs. General Alexander, we look forward to hearing what you're able to discuss in an open forum about how the data that you obtain from providers under the Business Records provision is used; and Deputy Attorney General Cole, we look forward to hearing more about the legal authorities themselves, and the state of the law on what privacy protections Americans' have in business records.

· One of the frustrating parts about being a member of this Committee is sitting at the intersection of classified intelligence programs and transparent democracy as representatives of the American people. The public trusts the government to protect the country from another 9/11 type attack, but that trust can start to wane when they are faced with inaccuracies, half truths and outright lies about the way intelligence programs are being run.

· One of the more damaging aspects of selectively leaking incomplete information is that it paints an inaccurate picture and fosters distrust in our government. This is particularly so when those of us who have taken an oath to protect information that can damage the national security if released, cannot publicly provide clarifying information because it remains classified. It is at times like these where our enemies within become almost as damaging as our enemies on the outside.

· It is critically important to protect sources and methods so we aren't giving the enemy our playbook. It is also important, however, to be able to talk about how these programs help protect us so that they continue to be reauthorized.

· General Alexander, you and I have talked over the past week about the need to be able to publicly elaborate on the success stories these authorities have contributed to without jeopardizing ongoing operations. I place the utmost value in protecting sources and methods, but I also recognize that when we are forced into the position of having to publicly discuss intelligence programs due to irresponsible, criminal behavior that we also have to carefully balance the need for secrecy with educating the public.

· I think you have struck the right balance between protecting sources and methods, and maintaining the public's trust—by providing more examples of how these authorities have helped disrupt terrorist plots and connections. And I appreciate your efforts in this regard.

· For these authorities to continue to work they must continue to be available. Without them, I fear we will return to the position we were in prior to the attacks of September 11, 2001. And that should be unacceptable to all of us.

· I hope today's hearing will help answer the questions that have arisen as a result of the fragmentary and distorted illegal disclosures over the past several days.

· Before recognizing General Alexander for his opening statement, I turn the floor over to the Ranking Member for any opening statement he would like to make.

The New York Times

July 6, 2013

In Secret, Court Vastly Broadens Powers of N.S.A.

By ERIC LICHTBLAU

WASHINGTON — In more than a dozen classified rulings, the nation's surveillance court has created a secret body of law giving the National Security Agency the power to amass vast collections of data on Americans while pursuing not only terrorism suspects, but also people possibly involved in nuclear proliferation, espionage and cyberattacks, officials say.

The rulings, some nearly 100 pages long, reveal that the court has taken on a much more expansive role by regularly assessing broad constitutional questions and establishing important judicial precedents, with almost no public scrutiny, according to current and former officials familiar with the court's classified decisions.

The 11-member Foreign Intelligence Surveillance Court, known as the FISA court, was once mostly focused on approving case-by-case wiretapping orders. But since major changes in legislation and greater judicial oversight of intelligence operations were instituted six years ago, it has quietly become almost a parallel Supreme Court, serving as the ultimate arbiter on surveillance issues and delivering opinions that will most likely shape intelligence practices for years to come, the officials said.

Last month, a former National Security Agency contractor, Edward J. Snowden, leaked a classified order from the FISA court, which authorized the collection of all phone-tracing data from Verizon business customers. But the court's still-secret decisions go far beyond any single surveillance order, the officials said.

"We've seen a growing body of law from the court," a former intelligence official said. "What you have is a common law that develops where the court is issuing orders involving particular types of surveillance, particular types of targets."

In one of the court's most important decisions, the judges have expanded the use in terrorism cases of a legal principle known as the "special needs" doctrine and carved out an exception to the Fourth Amendment's requirement of a warrant for searches and seizures, the officials said.

The special needs doctrine was originally established in 1989 by the Supreme Court in a ruling allowing the drug testing of railway workers, finding that a minimal intrusion on privacy was

justified by the government's need to combat an overriding public danger. Applying that concept more broadly, the FISA judges have ruled that the N.S.A.'s collection and examination of Americans' communications data to track possible terrorists does not run afoul of the Fourth Amendment, the officials said.

That legal interpretation is significant, several outside legal experts said, because it uses a relatively narrow area of the law — used to justify airport screenings, for instance, or drunken-driving checkpoints — and applies it much more broadly, in secret, to the wholesale collection of communications in pursuit of terrorism suspects. "It seems like a legal stretch," William C. Banks, a national security law expert at Syracuse University, said in response to a description of the decision. "It's another way of tilting the scales toward the government in its access to all this data."

While President Obama and his intelligence advisers have spoken of the surveillance programs leaked by Mr. Snowden mainly in terms of combating terrorism, the court has also interpreted the law in ways that extend into other national security concerns. In one recent case, for instance, intelligence officials were able to get access to an e-mail attachment sent within the United States because they said they were worried that the e-mail contained a schematic drawing or a diagram possibly connected to Iran's nuclear program.

In the past, that probably would have required a court warrant because the suspicious e-mail involved American communications. In this case, however, a little-noticed provision in a 2008 law, expanding the definition of "foreign intelligence" to include "weapons of mass destruction," was used to justify access to the message.

The court's use of that language has allowed intelligence officials to get wider access to data and communications that they believe may be linked to nuclear proliferation, the officials said. They added that other secret findings had eased access to data on espionage, cyberattacks and other possible threats connected to foreign intelligence.

"The definition of 'foreign intelligence' is very broad," another former intelligence official said in an interview. "An espionage target, a nuclear proliferation target, that all falls within FISA, and the court has signed off on that."

The official, like a half-dozen other current and former national security officials, discussed the court's rulings and the general trends they have established on the condition of anonymity because they are classified. Judges on the FISA court refused to comment on the scope and volume of their decisions.

Unlike the Supreme Court, the FISA court hears from only one side in the case — the

'government — and its findings are almost never made public. A Court of Review is empaneled to hear appeals, but that is known to have happened only a handful of times in the court's history, and no case has ever been taken to the Supreme Court. In fact, it is not clear in all circumstances whether Internet and phone companies that are turning over the reams of data even have the right to appear before the FISA court.

Created by Congress in 1978 as a check against wiretapping abuses by the government, the court meets in a secure, nondescript room in the federal courthouse in Washington. All of the current 11 judges, who serve seven-year terms, were appointed to the special court by Chief Justice John G. Roberts Jr., and 10 of them were nominated to the bench by Republican presidents. Most hail from districts outside the capital and come in rotating shifts to hear surveillance applications; a single judge signs most surveillance orders, which totaled nearly 1,800 last year. None of the requests from the intelligence agencies was denied, according to the court.

Beyond broader legal rulings, the judges have had to resolve questions about newer types of technology, like video conferencing, and how and when the government can get access to them, the officials said.

The judges have also had to intervene repeatedly when private Internet and phone companies, which provide much of the data to the N.S.A., have raised concerns that the government is overreaching in its demands for records or when the government itself reports that it has inadvertently collected more data than was authorized, the officials said. In such cases, the court has repeatedly ordered the N.S.A. to destroy the Internet or phone data that was improperly collected, the officials said.

The officials said one central concept connects a number of the court's opinions. The judges have concluded that the mere collection of enormous volumes of "metadata" — facts like the time of phone calls and the numbers dialed, but not the content of conversations — does not violate the Fourth Amendment, as long as the government establishes a valid reason under national security regulations before taking the next step of actually examining the contents of an American's communications.

This concept is rooted partly in the "special needs" provision the court has embraced. "The basic idea is that it's O.K. to create this huge pond of data," a third official said, "but you have to establish a reason to stick your pole in the water and start fishing."

Under the new procedures passed by Congress in 2008 in the FISA Amendments Act, even the collection of metadata must be considered "relevant" to a terrorism investigation or other intelligence activities.

The court has indicated that while individual pieces of data may not appear "relevant" to a terrorism investigation, the total picture that the bits of data create may in fact be relevant, according to the officials with knowledge of the decisions.

Geoffrey R. Stone, a professor of constitutional law at the University of Chicago, said he was troubled by the idea that the court is creating a significant body of law without hearing from anyone outside the government, forgoing the adversarial system that is a staple of the American justice system. "That whole notion is missing in this process," he said.

The FISA judges have bristled at criticism that they are a rubber stamp for the government, occasionally speaking out to say they apply rigor in their scrutiny of government requests. Most of the surveillance operations involve the N.S.A., an eavesdropping behemoth that has listening posts around the world. Its role in gathering intelligence within the United States has grown enormously since the Sept. 11 attacks.

Soon after, President George W. Bush, under a secret wiretapping program that circumvented the FISA court, authorized the N.S.A. to collect metadata and in some cases listen in on foreign calls to or from the United States. After a heated debate, the essential elements of the Bush program were put into law by Congress in 2007, but with greater involvement by the FISA court.

Even before the leaks by Mr. Snowden, members of Congress and civil liberties advocates had been pressing for declassifying and publicly releasing court decisions, perhaps in summary form.

Reggie B. Walton, the FISA court's presiding judge, wrote in March that he recognized the "potential benefit of better informing the public" about the court's decisions. But, he said, there are "serious obstacles" to doing so because of the potential for misunderstanding caused by omitting classified details.

Gen. Keith B. Alexander, the N.S.A. director, was noncommital when he was pressed at a Senate hearing in June to put out some version of the court's decisions.

While he pledged to try to make more decisions public, he said, "I don't want to jeopardize the security of Americans by making a mistake in saying, 'Yes, we're going to do all that.' "